UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS

EASTERN DIVISION

TRACY WITTMEYER, on behalf of herself and all others similarly situated, Plaintiff, v. HEARTLAND ALLIANCE FOR HUMAN NEEDS & HUMAN RIGHTS, HEARTLAND ALLIANCE HEALTH, HEARTLAND ALLIANCE INTERNATIONAL, LLC, HEARTLAND HOUSING, INC., AND HEARTLAND HUMAN CARE SERVICES, INC., Defendants.	Case No. 23-cv-1108

CLASS ACTION COMPLAINT

Plaintiff Tracy Wittmeyer, individually and on behalf of the Classes defined below of similarly situated persons ("Plaintiff"), alleges the following against Heartland Alliance for Human Needs & Human Rights, Heartland Alliance Health, Heartland Alliance International, LLC, Heartland Housing, Inc., and Heartland Human Care Services, Inc. (collectively, "Heartland" or "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against Heartland for its failure to properly secure and safeguard Plaintiff's and other similarly-situated Heartland clients' names, Social Security numbers, dates of birth, driver's license numbers, financial account numbers, medical and health information, or other sensitive records from hackers.

2. On information and belief, Heartland may have also left the same or similar personal information unsecured for its employees and independent contractors.

3. Heartland, based in Chicago, Illinois, is an anti-poverty organization that serves more than 500,000 people annually in the Midwest.

4. On or about December 15, 2022, Heartland posted a "Notice of Data Security Incident" on its website.

5. On or about December 19, 2022, Heartland filed official notice of a hacking incident with the Maine Attorney General.

6. On or about December 21, 2022, Heartland sent out letters to individuals whose information was compromised as a result of the incident.

7. Based on the information provided on the website, to the Maine Attorney General, and to Plaintiff, in or around late January 26, 2022, Heartland "experienced a disruption to its digital environment." In response, Heartland began an investigation through which it was revealed that an unauthorized party had access to certain files containing personal information (the "Data Breach").

8. Heartland waited nearly a full year from the initial discovery of the Data Breach to notify the public, its clients, and its employees and independent contractors that they were at risk. Heartland's delay is in violation of the Illinois Personal Information Protection Act, which requires that "[t]he disclosure notification shall be made in the most expedient time possible and without unreasonable delay." 815 Ill. Comp. Stat. § 530/10.

9. Additionally, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires a company to provide notice of a data breach impacting protected health information ("PHI") to every impacted individual "without unreasonable delay and in no case later than 60 days following discovery of the breach." 45 C.F.R. §§ 164.400-414.[1] Heartland did not comply with this HIPAA requirement.

10. Heartland itself also promises with regard to PHI that it will let impacted individuals "know promptly if a breach occurs that may have compromised the privacy or security of your information."[2]

11. As a result of this delayed response, Plaintiff and Class Members had no idea for an entire year that their information had been compromised, and that they were and continue to be at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes. This is especially problematic for low-income individuals like Plaintiff and Class Members who do not have the luxury of time or money to respond to fraudulent activity and identity theft.

12. Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. This includes names, Social Security numbers, dates of birth, driver's license numbers, financial account numbers, "some pieces of medical and health information" (collectively, the "Private Information") and additional personally identifiable information ("PII") and PHI that Heartland collected and maintained.

13. Armed with the Private Information accessed in the Data Breach and a head start, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing

[1] *Breach Notification Rule*, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Feb. 22, 2023).

[2] Heartland Alliance HIPAA Notice of Privacy Practices, https://www.heartlandalliance.org/wp-content/uploads/2022/12/Notice-of-Privacy-Practices.Participant-Layered_rev-1.pdf (last visited Feb. 22, 2023).

fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. Therefore, Plaintiff and Class Members have suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

15. Plaintiff brings this class action lawsuit to address Heartland's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their Private Information had been subject to the unauthorized access and what type of information was accessed. Indeed, the notice to Plaintiff only informed her what personal information "may have been accessed."

16. The potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Heartland, and thus Heartland was on notice that failing to take necessary steps to secure the Private Information left that Private Information vulnerable to an attack.

17. On information and belief, Heartland and its employees failed to properly monitor the computer network and systems that housed the Private Information. On information and belief, had Heartland properly monitored its networks, it would have discovered the Data Breach sooner.

18. Plaintiff's and Class Members' identities are now at risk because of Heartland's negligent conduct, as the Private Information that Heartland collected and maintained is now likely in the hands of data thieves and unauthorized third-parties. Even though Heartland is a non-profit entity with admirable social goals, it still knowingly collected Plaintiff's and Class Members' Personal Information, and the damage caused to Plaintiff and the Class Members here is the same as in any data breach. Therefore, Heartland is obligated to make Plaintiff and the Class Members whole for the damage it caused.

19. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

20. Plaintiff seeks remedies here including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Heartland's data security systems, future annual audits, and adequate credit monitoring services funded by Heartland.

PARTIES

21. Plaintiff Tracy Wittmeyer is, and at all times mentioned herein was, an individual citizen of the State of Illinois residing in the City of Lakemoor in McHenry County.

22. Defendant Heartland Alliance for Human Needs & Human Rights is an anti-poverty organization with its principal place of business in Chicago, Illinois in Cook County.

23. Defendant Heartland Alliance Health is a non-profit organization that provides health services with its principal place of business in Chicago, Illinois in Cook County.

24. Defendant Heartland Alliance International, LLC is a non-profit organization with a principal place of business in Chicago, Illinois in Cook County that provides mental health and psychosocial support services.

25. Defendant Heartland Housing, Inc. is a non-profit organization with a principal place of business in Chicago, Illinois in Cook County that develops and manages affordable housing.

26. Defendant Heartland Human Care Services, Inc. is a non-profit organization with a principal place of business in Chicago, Illinois in Cook County that develops and manages affordable housing.

JURISDICTION AND VENUE

27. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many

of whom have different citizenship from Heartland, including residents of states as far away as Maine and Montana. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

28. This Court has jurisdiction over the Defendants because Heartland operates in and has its principal place of business in this District.

29. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Heartland has harmed Class Members residing in this District.

HEARTLAND COLLECTS HIGHLY SENSITIVE INFORMATION

30. Heartland is a group of not-for-profit organizations based in Chicago, Illinois. Founded in 1888, Heartland is one of the Midwest's largest anti-poverty organizations. Heartland employs more than 1,600 people and generates over $100 million in annual revenue.

31. As a condition of receiving services, Heartland requires that its clients entrust it with highly sensitive personal information. In the ordinary course of receiving service from Heartland, clients are required to provide sensitive personal information such as names, Social Security numbers, dates of birth, driver's license numbers, and financial account numbers, among other things. For those clients that receive services through Heartland Alliance Health or other health programs that Heartland provides, Heartland also collects and maintains PHI for them. On information and belief, Heartland also maintains similar personal information for its employees and independent contractors.

32. Heartland uses information from its clients, *inter alia*, to provide job training and educational opportunities, to provide health and healing services, and/or to provide legal services as part of specialized resettlement services.

33. In its Privacy Policy effective December 9, 2022, Heartland promises its clients that it will only share personal information in specific situations, such as to comply with the law or with third-party providers such as credit card payment processors.[3]

[3] *See* Heartland Alliance Privacy Policy, https://www.heartlandalliance.org/about/privacy-policy/ (last visited Feb. 22, 2023).

34. Pursuant to HIPAA, Heartland also maintains a Notice of Privacy Practices ("HIPAA Privacy Notice").[4] In that notice, it promises its clients that:

a. "We are required by law to maintain the privacy and security of your protected health information."

b. "We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."

c. "We will not use or share your information other than as described here unless you tell us we can in writing."

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Heartland assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

36. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

37. Plaintiff and Class Members relied on Heartland to keep their Private Information confidential and securely maintained and to make only authorized disclosures of this information.

HEARTLAND'S DATA BREACH AND NOTICE

38. Plaintiff was a client of Heartland. As part of receiving services from Heartland, Heartland collected, *inter alia*, her name, date of birth, Social Security number, and medical and health information.

39. According to Heartland, on or around January 26, 2022, Heartland learned of unauthorized access to its computer systems. An unauthorized individual or individuals accessed a cache of highly sensitive PII and PHI, including names, dates of birth, Social Security numbers, driver's license numbers, financial account numbers, and medical and health information.

[4] https://www.heartlandalliance.org/wp-content/uploads/2022/12/Notice-of-Privacy-Practices.Participant-Layered_rev-1.pdf (last visited Feb. 22, 2023).

40. In mid-to-late December 2022, nearly a full year after Heartland learned that the Class's Private Information was first accessed by cybercriminals, Heartland finally began to notify its clients, employees, and independent contractors that its investigation identified that their Private Information was breached in a "data security incident." The notice to Plaintiff stated that "[t]he potentially accessed information may have included your name, Social Security number, date of birth, [and] some pieces of medical or health information such as diagnosis, medication and medication monitoring notes, other health care provider and case manager notes, and, for dental patients, dental scans." On information and belief, other Class Members received the same or similar notice.

41. The notice letter then attached pages entitled "Steps You Can Take to Protect Your Personal Information," which listed steps that data breach victims can take, such as reviewing their account statements, notifying law enforcement of suspicious activity, getting a copy of a free credit report, and placing a fraud alert on a credit report. Other than offering 12 or 24 months of credit monitoring and identity protection services (that impacted individuals would need to affirmatively sign up for on or before March 15, 2023) and a call center number that victims could contact if they had "questions or need assistance," Heartland offered no other substantive steps to help victims like Plaintiff and Class Members protect themselves.

42. Heartland had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

43. Plaintiff and Class Members provided their Private Information to Heartland with the reasonable expectation and mutual understanding that Heartland would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of security breaches.

44. Heartland's data security obligations were particularly important given the substantial increase in cyberattacks. Indeed, Heartland knew that it serves a low-income population

that is unlikely to have the knowledge or resources to protect themselves from the negative repercussions caused by Heartland's failure to safeguard their Private Information.

45. Heartland knew or should have known that its electronic records would be targeted by cybercriminals.

HEARTLAND FAILED TO COMPLY WITH FTC GUIDELINES

46. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

47. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

48. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

49. The FTC has brought enforcement actions against entities for failing to adequately and reasonably protect data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting

from these actions further clarify the measures businesses must take to meet their data security obligations.

50. On information and belief, Heartland failed to properly implement basic data security practices. Heartland's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

51. Heartland was at all times fully aware of its obligation to protect the PII of its clients.

THE DANGERS INVOLVED WITH PHI

52. While PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200,[5] PHI can sell for as much as $363 according to the Infosec Institute.[6] This is because one's personal health history cannot be changed unlike credit card information.

53. PHI has increased value because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can also be used to create fake insurance claims, allowing for the purchase and resale of medical equipment. Some criminals use PHI to illegally gain access to prescriptions for their own use or resale.

54. Because of the value of PHI, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

55. Cyberattacks and data breaches at healthcare providers like Heartland are especially problematic because they can negatively impact the overall daily lives of patients affected by the attack. Researchers have found that among healthcare providers that experience a data security

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 22, 2023).

[6] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited Feb. 22, 2023).

incident, the death rate among patients increased in the months and years after the incident.[7] Researchers have also found that at healthcare providers that experienced a data security incident, the incident was associated with an overall deterioration in timeliness and patient outcomes.[8]

HEARTLAND FAILED TO COMPLY WITH INDUSTRY STANDARDS

56. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

57. Some industry best practices that should be implemented by entities like Heartland, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. Upon information and belief, Defendants failed to follow some or all of these industry best practices.

58. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. Upon information and belief, Defendants failed to follow these cybersecurity best practices, including failure to train their staff.

59. Upon information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-

[7] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptickin-fatal-heart-attacks (last visited Feb. 22, 2023).

[8] *See* Sung J. Choi, *et al.*, *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Feb. 22, 2023).

2), the HIPAA Security Rule and Breach Notification Rule, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness. Upon information and belief, Defendants' failure to comply with these accepted standards opened the door to the cyber incident resulting in the Data Breach.

HEARTLAND'S SECURITY OBLIGATIONS AND ITS VIOLATIONS OF HIPAA

60. Heartland breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data.

61. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

62. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling the types of data that Defendants left unguarded. The HHS subsequently promulgated multiple regulations.

63. Cyberattacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.10.

64. Heartland's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect its clients', employees', and independent contractors' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of PII and PHI;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of Section 5 of the FTCA;

f. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

g. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption")

h. Failing to provide prompt notice of the Data Breach to its clients, employees, and independent contractors; and

i. Failing to adhere to industry standards for cybersecurity.

65. On information and belief, as a result of computer systems in need of security upgrades, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Heartland negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

66. Accordingly, Plaintiff's and Class Members' lives have been severely disrupted. What's more, they now face an increased risk of fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Heartland.

DATA BREACHES, FRAUD, AND IDENTITY THEFT

67. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.9 Exposure of personal information that a consumer wishes to keep private may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

68. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

69. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if

[9] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited Feb. 22, 2023).

someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[10]

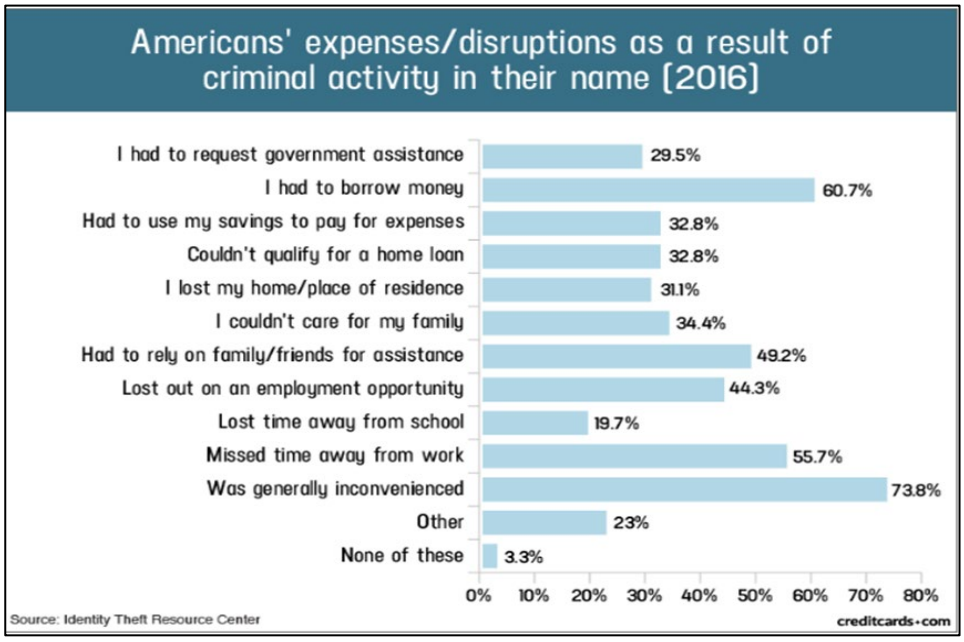
70. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

71. Identity thieves can also use Social Security numbers to obtain an official identification card in the victim's name but with the thief's picture, use the victim's name and Social Security number to obtain government benefits, or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

72. A study by the Identity Theft Resource Center[11] shows the multitude of harms caused by fraudulent use of PII:

[10] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Feb. 22, 2023).

[11] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Feb. 22, 2023).



73. Moreover, the value of Private Information is axiomatic. The consequences of cyberthefts include heavy prison sentences. The fact that identity thieves attempt to steal identities notwithstanding these possible heavy prison sentences illustrates beyond a doubt that Private Information has considerable market value.

74. Theft of PHI is particularly troubling and can result in medical identity theft, where a thief uses the victim's information to see a doctor, get prescription drugs, buy medical devices, submit insurance claims, or get other medical care.12 If the thief's health information is mixed with the victim's health information, it can negatively impact the victim's health insurance benefits and credit.

75. Additionally, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data

[12] *What To Know About Medical Identity Theft*, Federal Trade Commission (May 2021), *available at* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Feb. 22, 2023).

breach victims themselves. Insurance companies purchase and use wrongfully-disclosed PHI to adjust their insureds' medical insurance premiums.

76. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:13

77. [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

78. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

79. As a result, there is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice now but to vigilantly monitor their accounts for many years to come.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

80. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

81. Plaintiff's Private Information, including sensitive PII and PHI, was compromised as a direct and proximate result of the Data Breach.

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Feb. 22, 2023).

82. As a direct and proximate result of Heartland's conduct, Plaintiff and Class Members have suffered an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. This is especially problematic for low-income individuals like Plaintiff and Class Members who do not have the luxury of time or money to respond to fraudulent activity and identity theft.

83. As a direct and proximate result of Heartland's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

84. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

85. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information, as potential fraudsters could use that information to target their schemes more effectively to Plaintiff and Class Members.

86. Plaintiff and Class Members also face substantial risk of being victims of medical identity theft.

87. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

88. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages.

89. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their accounts and records for misuse.

90. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

91. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Heartland, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to making sure that the storage of data or documents containing personal information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

92. As a direct and proximate result of Heartland's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and either have suffered harm or are at an increased risk of future harm.

CLASS ALLEGATIONS

93. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and on behalf of all other persons similarly situated (the "Class").

94. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Illinois Subclass

All residents of Illinois who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

95. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

96. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

97. Each of the proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

98. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of approximately 54,914 clients, employees, and independent contractors of Heartland whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Heartland's records, Class Members' records, publication notice, self-identification, and other means.

99. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Heartland engaged in the conduct alleged herein;

b. Whether Heartland's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act , invoked below;

c. When Heartland actually learned of the Data Breach and whether its response was adequate;

d. Whether Heartland unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether Heartland failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Heartland's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Heartland's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Heartland owed a duty to Class Members to safeguard their Private Information;

i. Whether Heartland breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Heartland had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Heartland breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Heartland knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of Heartland's misconduct;

o. Whether Heartland's conduct was negligent;

p. Whether Heartland's conduct was *per se* negligent;

q. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

r. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiff and the Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

100. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

101. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

102. Predominance. Heartland has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Heartland's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

103. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Heartland. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

104. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Heartland has acted or has refused to act on grounds generally applicable to the Class so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

105. Finally, all members of the proposed Class are readily ascertainable. Heartland has access to the names and addresses of Class Members affected by the Data Breach, which it says that it gathered in order to notify clients and employees who were impacted. Accordingly, Class Members have already been preliminarily identified and sent notice of the Data Breach by Heartland.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE ILLINOIS STATE SUBCLASS)

106. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

107. Heartland knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

108. Heartland's duty included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

109. Heartland knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Heartland was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks, especially because it maintained PHI.

110. Heartland owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Heartland's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the Illinois Consumer Fraud and Deceptive Business Practices Act and HIPAA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach and to precisely disclose the type(s) of information compromised.

111. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

112. Heartland's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants were bound by industry standards to protect confidential Private Information.

113. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Heartland, and Heartland owed them a duty of care to not subject them to an unreasonable risk of harm.

114. Heartland, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Heartland's possession.

115. Heartland, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

116. Heartland, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

117. Heartland breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
b. Failing to adequately monitor the security of its networks and systems;
c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;
d. Allowing unauthorized access to Class Members' Private Information;
e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

118. Heartland acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach so that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

119. Heartland had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Heartland with their Private Information was predicated on the understanding that Heartland would take adequate security precautions. Moreover, only Heartland had the ability to protect its systems (and the Private Information that it stored on them) from attack.

120. Heartland's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

121. Heartland's breaches of duty caused a foreseeable risk to Plaintiff and Class Members that they would be harmed by suffering from identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

122. As a result of Heartland's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

123. Heartland also had independent duties under state laws like Illinois' and under HIPAA that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

124. As a direct and proximate result of Heartland's negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of further harm.

125. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was reasonably foreseeable.

126. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was the direct and proximate result of Heartland's negligent conduct.

127. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

128. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Heartland to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE ILLINOIS STATE SUBCLASS)

129. Plaintiff restates and realleges the allegations in paragraphs 1-105 as if fully set forth herein.

130. Pursuant to Section 5 of the FTCA, Heartland had a duty to provide fair and adequate computer systems and data security to safeguard Plaintiff's and Class Members' Private Information.

131. Heartland breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA and its obligations under HIPAA, including but not limited to: proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

132. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

133. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect Private Information. The FTC publications described above and the industry-standard cybersecurity measures also form part of the basis of Heartland's duty in this regard.

134. Pursuant to HIPAA, Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' PHI.

135. Under HIPAA, Defendants had a duty to render electronic PHI into unusable, unreadable, or indecipherable form. *See* 45 C.F.R. § 164.304.

136. Heartland violated the FTCA and HIPAA by failing to use reasonable measures to protect Private Information of Plaintiff and Class Members and by not complying with applicable industry standards, as described herein.

137. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Heartland's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Private Information.

138. Heartland's violations of the FTCA and HIPAA constitute negligence *per se*.

139. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Heartland's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

140. As a direct and proximate result of Heartland's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information (including PII) because of the Data Breach, including but not limited to damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

141. Heartland breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

142. As a direct and proximate result of Heartland's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

143. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Heartland to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE ILLINOIS SUBCLASS)

144. Plaintiff restates and realleges the allegations in paragraphs 1-105 as if fully set forth herein.

145. Plaintiff and Class Members entered into a valid and enforceable contract through which Heartland provided services to Plaintiff and Class Members. That contract included promises by Defendants to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

146. Heartland's Privacy Policy and HIPAA Privacy Notice memorialized the rights and obligations of Heartland and its clients. In those documents, Heartland commits to protecting the privacy and security of personal information, promises to never share such information except under certain limited defined circumstances, and assures prompt notification of any data breach.

147. Heartland promised to comply with all HIPAA standards, state and federal law, and to ensure Plaintiff's and Class Members' PHI was protected, secured, kept private, and not disclosed.

148. Plaintiff and Class Members fully performed their obligations under their contracts with Heartland.

149. However, Heartland did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore Heartland breached its contract with Plaintiff and Class Members.

150. Heartland allowed third parties to access, copy, and/or transfer Plaintiff's and Class Members' Private Information without permission. Therefore, Heartland breached the Privacy Policy and HIPAA Privacy Notice with Plaintiff and Class Members.

151. Heartland's failure to satisfy its confidentiality and privacy obligations resulted in Heartland providing services to Plaintiff and Class Members that were of a diminished value.

152. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein.

153. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Heartland to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE ILLINOIS STATE SUBCLASS)

154. Plaintiff restates and realleges the allegations in paragraphs 1-105 as if fully set forth herein.

155. This Count is pleaded in the alternative to Count III above.

156. Heartland provides various services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendants regarding the provision of those services through their collective conduct.

157. Through Defendants' provision of services, they knew or should have known that they must protect Plaintiff's and Class Members' confidential Private Information in accordance with Heartland's policies, practices, and applicable law.

158. As part of receiving services, Plaintiff and Class Members turned over valuable PII and PHI to Heartland. Accordingly, Plaintiff and Class Members bargained with Heartland to securely maintain and store their Private Information.

159. Heartland violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

160. Plaintiff and Class Members have been damaged by Heartland's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
(ON BEHALF OF PLAINTIFF AND THE ILLINOIS SUBCLASS)

161. Plaintiff restates and realleges the allegations in paragraphs 1-105 as if fully set forth herein.

162. As fully alleged above, Defendants engaged in unfair and deceptive acts and practices in violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. § 505/1, *et seq*.

163. Reasonable individuals would be misled by Defendants' misrepresentations and/or omissions concerning the security of their PII and PHI, because they assume entities that collect and maintain PII and PHI will properly safeguard that PII and PHI in a manner consistent with industry standards and practices.

164. Heartland did not inform Plaintiff and Class Members that it failed to properly safeguard their Private Information, thus misleading Plaintiff and Class Members in violation of Ill. Comp. Stat. § 505/1, *et seq*. Such misrepresentation was material because Plaintiff and Class Members entrusted Heartland with their Private Information.

165. Had Plaintiff and Class Members known of Heartland's failure to maintain adequate security measures to protect their Private Information, Plaintiff and Class Members would not have entrusted their Private Information to Heartland.

166. Heartland engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the provision of and advertisement of their services in violation of the Illinois Consumer Fraud and Deceptive Business

Practices Act, including: (a) failing to maintain adequate data security to keep Plaintiff's and Class Members' Private Information from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTCA; (b) failing to disclose or omitting material facts to Plaintiff and Class Members regarding Defendants' lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiff and Class members; (c) failing to disclose or omitting material facts to Plaintiff and Class Members about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Private Information of Plaintiff and Class Members; and (d) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Class Members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

167. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and their failure to comply with applicable state and federal laws and industry standards would be unknown and not easily discoverable by Plaintiff and Class Members and would defeat Plaintiff's and Class Members' reasonable expectation about the security of their Private Information.

168. Defendants intended that Plaintiff and Class Members would rely on their deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' provision of services.

169. Defendants' wrongful practices were and are injurious to the public because those practices were part of Heartland's generalized course of conduct that applied to Plaintiff and Class Members. Plaintiff and Class Members have been adversely affected by Heartland's conduct and the public was and is at risk thereof.

170. Heartland also violated 815 Ill. Comp. Stat. § 505/2 by failing to immediately notify Plaintiff and Class Members of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. § 530/1.

171. As a result of Heartland's wrongful conduct, Plaintiff and Class Members were injured in that they would not have provided their Private Information to Heartland had they known or been told that Heartland failed to maintain sufficient security to keep their Private Information from being hacked and taken and misused by others.

172. As a direct and proximate result of Heartland's violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, Plaintiff and Class Members have suffered harm, including identity theft, harm resulting from damaged credit scores and information, loss of time and money obtaining protections against future identity theft, loss of time and money resolving fraudulent charges, unreimbursed losses related to fraudulent charges, and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Private Information, entitling them to damages in an amount to be proven at trial.

173. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and Class Members seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Heartland's violations of the Illinois Consumer Fraud and Deceptive Business Practices Act.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE ILLINOIS STATE SUBCLASS)

174. Plaintiff restates and realleges the allegations in paragraphs 1-105 as if fully set forth herein.

175. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

176. Heartland owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Private Information.

177. Heartland still possesses Private Information regarding Plaintiff and Class Members.

178. Plaintiff alleges that Heartland's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and the risk remains that further compromises of her Private Information will occur in the future.

179. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Heartland owes a legal duty to secure Class Members' Private Information and to timely notify them of a data breach under the common law, Section 5 of the FTCA, and HIPAA;

b. Heartland's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect Private Information; and

c. Heartland continues to breach this legal duty by failing to employ reasonable measures to secure Class Members' Private Information.

180. This Court should also issue corresponding prospective injunctive relief requiring Heartland to employ adequate security protocols consistent with legal and industry standards to protect its clients', employees', and independent contractors' Private Information, including the following:

a. Order Heartland to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that to comply with Defendants' explicit or implicit contractual obligations and duties of care, Heartland must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,

penetration tests, and audits on Heartland's systems on a periodic basis, and ordering Heartland to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Heartland's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting training and education to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its clients, employees, and independent contrctors about the threats they face with regard to the security of their Private Information, as well as the steps they must take to protect themselves.

181. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury and lack an adequate legal remedy to prevent another data breach at Heartland. The risk of another such breach is real, immediate, and substantial. If another breach at Heartland occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

182. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Heartland if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other related damages. On the other hand, the cost of Heartland's compliance with an injunction requiring reasonable prospective data security

measures is relatively minimal, and Heartland has a pre-existing legal obligation to employ such measures.

183. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Heartland, thus preventing future injury to Plaintiff and Class Members whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Classes requested herein;

b. Judgment in favor of Plaintiff and Class Members, awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order instructing Heartland to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Heartland to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: February 22, 2023

Respectfully submitted,

/s/ Mason A. Barney

SIRI & GLIMSTAD LLP
Mason A. Barney (Bar No. 4405809)
Steven D. Cohen (*pro hac vice* to be filed)
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: scohen@sirillp.com